Der EuGH erklärt Safe-Harbour für ungültig – Was folgt daraus für die europäischen Sicherheitsbehörden?

Gastautor 2015-10-13T12:01:58

von EMMA PETERS

Im Hinblick auf die Auswirkungen der Schrems-Entscheidung des EuGH sind die innereuropäischen Implikationen und ihr Einfluss auf die transatlantische Datenschutzdebatte bisher wenig beleuchtet worden – und das obwohl Max Schrems, der Kläger des Ausgangsverfahrens, bereits unmittelbar nach der Urteilsverkündung prophezeit hat, dass dieses Urteil auch für die Regelungen und Praktiken innereuropäischer Überwachung Folgen haben werde. Ist das tatsächlich so? Oder fordert der EUGH von den USA Beschränkungen im nationalen Sicherheitsrecht, die er von den EU-Mitgliedsstaaten nicht verlangen kann? Wirkt sich das Urteil auf die Überwachung von Nicht-Unionsbürgern durch EU-Staaten im Ausland aus? Was folgt daraus für die Datenschutzdiskussion zwischen der EU und den USA?

Gelten die Vorgaben des EuGH auch für die europäischen Sicherheitsbehörden?

Der EuGH hat die Anforderungen der Grundrechtecharta an den Datenschutz – insbesondere im Hinblick auf den staatlichen Datenzugriff zu Sicherheitszwecken – konkretisiert und bestärkt. Die Entscheidung bezog sich jedoch allein auf die Frage, wann in einem Drittland ein dem Unionsschutz gleichwertiges Datenschutzniveau vorherrsche. Gelten diese Vorgaben auch für den Zugriff der mitgliedsstaatlichen Behörden auf Daten in Unternehmensdatenbanken? Wohl nicht. Denn die Unionsgrundrechte finden auf diese Maßnahmen keine Anwendung. Das klingt paradox, oder!? Kann es wirklich sein, dass die Unionsgrundrechte von einem Drittland wie den USA – wenn auch nur mittelbar – ein bestimmtes Maß an Schutz

von Daten der Unionsbürger verlangen, das sie von den Sicherheitsbehörden der EU-Mitgliedsstaaten nicht einfordern können?

Dieses Ergebnis hängt mit der Regelung zur Anwendbarkeit der Unionsgrundrechte zusammen. Nach Art. 51 Abs. 1 EUGRCh gelten diese nämlich grundsätzlich für die EU-Organe, „für die Mitgliedsstaaten ausschließlich bei der Durchführung des Rechts der Union“. Im Bereich der inneren Sicherheit verfügt die Union jedoch immer noch nur über sehr eingeschränkte Kompetenzen. So beschränken sich die Art. 67 ff. AEUV auf die Regelung der behördlichen und justiziellen *Zusammenarbeit* in Strafsachen – zu der auch der Informations*austausch* gehört (vgl. Art. 87 Abs. 1 und 2 lit. a AEUV), nicht jedoch der Zugriff der Behörden auf die Daten beim Privaten. Art. 72 AEUV bestärkt den Ausnahmecharakter unionsrechtlicher Kompetenzen im Raum der Freiheit, der Sicherheit und des Rechts (RFSR). Ebenso verpflichtet Art. 4 Abs. 2 EUV die Union bei der Ausübung ihrer Kompetenzen zur Achtung der grundlegenden Staatsfunktionen, insbesondere „die Aufrechterhaltung der öffentlichen Ordnung“; in Satz 3 ist ein mitgliedsstaatlicher Zuständigkeitsvorbehalt für die nationale Sicherheit festgeschrieben.
Die Wahrung der öffentlichen und nationalen Sicherheit – auch durch Zugriff auf Unternehmensdatenbanken – fällt somit weitgehend bzw. ausschließlich in die Zuständigkeit der Mitgliedsstaaten. Dementsprechend stellen nationale Maßnahmen in diesem Bereich in der Regel keine Durchführung von Unionsrecht dar und eröffnen somit auch nicht den Anwendungsbereich der Unionsgrundrechte. Diese könnten nur über ein anderes ‚Einfallstor‘ – die Durchführung anderer unionsrechtlicher Regelungen – zur Anwendung gelangen. Angesichts der weiten Auslegung des Begriffs „Durchführung des Rechts der Union“ i. S. d. Art. 51 Abs. 1 EUGRCh durch den EuGH (siehe Rs. Åkerberg Fransson) würden bereits gewisse Berührungspunkte mit anderen Sekundärrechtsakten der EU für ein solches ‚Einfallstor’ ausreichen.

In seiner Entscheidung zu Safe-Harbour erklärte der EuGH die Datenschutzrichtlinie 95/46 (insbesondere ihren Art. 25 zur Angemessenheitsfeststellung) zu einem solchen ‚Einfallstor‘ für die Unionsgrundrechte im Hinblick auf das US-Recht: diese ‚mittelbare Einwirkungsmöglichkeit‘ folgte daraus, dass das Verfahren primär die Zulässigkeit der Datenübertragung von einem EU-Unternehmen in Drittland – und nicht sicherheitsrechtliche Zugriffsmaßnahmen – zum Gegenstand hatte. Damit war der Anwendungsbereich der Richtlinie eröffnet. Denn Art. 25 der Richtlinie lässt eine Übermittlung personenbezogener Daten in ein Drittland nur zu, wenn dieser Staat *tatsächlich* ein angemessenes Schutzniveau der Grundrechte gewährleistet, das dem in der Unionsrechtsordnung garantierten Niveau gleichwertig ist. Anschließend erklärte das Gericht die Unionsgrundrechte zum materiellen Maßstab für die Prüfung, ob das US-Recht ein gleichwertiges Datenschutzniveau gewährleiste. Diese Prüfung betraf die gesamte US-Rechtsordnung und bezog auch ihre Regelungen zum staatlichen Datenzugriff zu Sicherheitszwecken mit ein.

Könnte die Richtlinie 95/46 auch ein ‚Einfallstor' für die Anwendbarkeit auf eine gleich gelagerte Maßnahmen der Mitgliedsstaaten sein?

Anders als bei der Schrems-Entscheidung bleibt die ‚mittelbare Einwirkungsmöglichkeit' über die vorherige private Datenübermittlung an ein EU-Unternehmen, auf dessen Daten anschließend zugegriffen werden, verschlossen. Denn die Übermittlung in einen EU-Mitgliedsstaat setzt keine Angemessenheitsprüfung voraus. Auf eine unmittelbare Prüfung einer sicherheitsrechtlichen Maßnahme – den sicherheitsbehördlichen Zugriff auf personenbezogene Daten beim Unternehmen – fände diese Richtlinie schon grundsätzlich keine Anwendung. Art. 3 Abs. 1 der Richtlinie schließt nämlich die Verarbeitung von Daten betreffend die öffentliche Sicherheit und die Sicherheit des Staates ausdrücklich aus dem Anwendungsbereich aus.

Etwas anderes ergäbe sich wohl auch nicht aus dem Rückgriff auf den Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. Dieser ist ausdrücklich – entsprechend der oben dargelegten Kompetenzen im RFSR, die sich auf die mitgliedsstaatliche Zusammenarbeit beschränken – nur auf den Daten*austausch* anwendbar.

Zwischenfazit

Demnach gibt es kein ‚Einfallstor' für die Unionsgrundrechte im Hinblick auf die mitgliedsstaatliche Erhebung personenbezogener Daten zu Sicherheitszwecken. Dabei erscheint es angesichts des Auseinanderfallens von unionsgrundrechtlichen Datenschutzanforderungen und Kompetenzgrundlagen der EU im RFSR sehr fraglich, ob überhaupt eine taugliche primärrechtliche Kompetenzgrundlage für eine grundrechtskonforme Regelung das mitgliedsstaatlichen Datenzugriffs zu Sicherheitszwecken zur Verfügung stünde.

Der EuGH stellt also (nicht durchsetzbare, aber für eine positive Angemessenheitsentscheidung i. S. d. Art. 25 der Richtlinie 95/46 erforderliche) Anforderungen an den staatlichen Zugriff auf Daten von Unionsbürgern, die von EU-Unternehmen an Unternehmen im Drittland übermittelt wurden – deren Einhaltung er jedoch von den mitgliedsstaatlichen Behörden nicht verlangen kann. Dies lässt daran zweifeln, ob der Zugriff (seitens der US-Behörden) auf die in die USA übermittelten Daten überhaupt – wie vom EuGH ohne Begründung angenommen – tauglicher Anknüpfungspunkt der Angemessenheit des Datenschutzniveaus sein kann. Denn selbst wenn die Unionsgrundrechte dieses Schutzlevel vorgeben – sie können es weder bei den Unionsorganen und -einrichtungen (die grundsätzlich keine direkten Zugriffsbefugnisse zu Sicherheitszwecken haben) noch in den Mitgliedsstaaten durchsetzen.

Auswirkungen auf Zugriffsbefugnisse innereuropäischer Sicherheitsbehörden außerhalb der EU und auf Nicht-Unionsbürger?

Doch selbst wenn diese Anforderungen auf die mitgliedsstaatlichen Sicherheitsbehörden Anwendung fänden: gälte dies nur im Hinblick auf die Überwachung von Unionsbürgern bzw. von Personen, die sich in der EU aufhalten? Oder auch darüber hinaus? Bei aller Zustimmung zu den strengen Anforderungen, die der EuGH nun den USA zugunsten des Schutzes personenbezogener Daten der Unionsbürger (auch) bei der sicherheitsbehördlichen Überwachung auferlegt: ist denn der Schutz von US-Bürgern vor europäischer Auslandsüberwachung ausgereifter?

Auch daran kann man zweifeln: So hat sich der EuGH (noch) nicht zur extraterritorialen Anwendbarkeit der Unionsgrundrechte auf Nicht-Unionsbürger geäußert. Auch die Rechtsprechung des EGMR lässt eine extraterritoriale Anwendbarkeit der EMRK nur in sehr eingeschränkten Fällen zu. Es ist darüber hinaus gleichermaßen unklar, wie die mitgliedsstaatlichen Behörden ihre nationale Grundrechtsbindung gegenüber Daten bezogen auf Nicht-EU-Bürger einschätzen, selbst wenn sie diese Daten bei inländischen Unternehmen erheben. So vertritt zum Beispiel der BND die Rechtsauffassung, dass die Grundrechte bei der Überwachung im „offenen Himmel“, wie die Ausspähung von Nicht-Deutschen bzw. Nicht-Unionsbürgern im Ausland genannt wird, keine Anwendung fänden.

Fazit: Ist es nicht ein wenig vermessen, von den USA zu verlangen, was man selbst nicht einhält?

Der transatlantische „Clash“ bei der Balance von persönlicher Freiheit und innerer Sicherheit hat eine neue Eskalationsstufe erklommen. Zurzeit ist noch nicht abzusehen, welche Kompromisse dazu gefunden werden. Sicher ist aber, dass eine Lösung nur im Dialog entstehen kann. Der EuGH ist mit dem Schrems-Urteil vorgeprescht und verlangt von den USA einen Schutzstandard für die Daten der Unionsbürger, den er von seinen eigenen Mitgliedsstaaten nicht verlangen kann – und die diese den US-Bürgern nach derzeitigem Kenntnisstand auch ihrerseits nicht zukommen lassen. Das ist nicht nur rechtlich zweifelhaft, sondern bringt die EU bzw. ihre Mitgliedsstaaten gerade im Hinblick auf die Verhandlungen eines neuen Safe-Harbour-Abkommens in eine schwierige Position. Vor diesem Hintergrund sind die EU bzw. ihre Mitgliedsstaaten, wollen sie ihrer (Rechts-)Auffassung international politisches Gewicht verleihen, gut beraten, erst einmal ‚vor ihrer eigenen Tür zu kehren‘ und im Recht der inneren Sicherheit einen EU-weit einheitlichen, hohen Schutzstandard – auch für Nicht-Unionsbürger – zu etablieren.
